REMARKS

Reconsideration and allowance of the present application are respectfully requested. Claims 1-33 remain pending in the application. By this Amendment claims 2, 5, 11, 18, 19, 22-24 and 27-31 are amended.

In numbered paragraph 2, page 2 of the Office Action, claims 1-15, 19, 22-24 and 26-33 are rejected as being anticipated by U.S. Patent 6,301,658 (Koehler). In numbered paragraph 4, page 13 of the Office Action, dependent claims 16-18 are rejected as being unpatentable over Koehler in view of U.S. Patent 4,264,782 (Konheim). In numbered paragraph 5, page 14 of the Office Action, dependent claims 20 and 21 are rejected as being unpatentable over the Koehler patent in view of U.S. Patent 5,903,651 (Kocher). In numbered paragraph 6, page 16 of the Office Action, dependent claim 25 is rejected as being unpatentable over the Koehler patent in view of U.S. Patent 5,818,955 (Smithies et al.). These rejections are respectfully traversed.

Applicants have disclosed a Certificate Status Service that is configurable, directed, and able to retrieve status from any approved Certification Authority (CA) is disclosed. The CSS may be used by a trusted third-party repository of information objects and comparable systems or applications whose roles are validating the right of an individual to perform a requisite action, the authenticity of submitted electronic information objects, and the status of authentication certificates used in digital signature verification and user authentication processes. The validity check on authentication certificates is performed by querying an issuing CA. Traditionally, to create a trusted Public Key Infrastructure (PKI) needed to validate certificates, complex relationships are formed by cross-certification among CAs or by use of PKI

bridges. The PKI and CA interoperability problem is addressed from a different point of view, with a focus on establishing a trust environment suitable for the creation, execution, maintenance, transfer, retrieval and destruction of electronic original information objects that may also be transferable records (ownership may change hands). A trusted third-party repository of information objects is concerned only with a known set of "approved CAs" although they may support a multitude of business environments, and within that set of CAs, only with those certificates that are associated with trusted third-party repository of information objects user accounts. Building PKI/CA trusted relationships is not required as the CSS achieves a trusted environment by querying only approved CAs and maintaining caches of valid certificates' status.

The foregoing features are broadly encompassed by claim 1, which recites a method of providing a Certificate Status Service ("CSS") for checking validities of authentication certificates issued by respective issuing Certification Authorities ("CAs"), including the steps of: identifying information needed for retrieving a status of an authentication certificate from an issuing CA that issued the authentication certificate; configuring a connector based on the identified information for communicating with the issuing CA; communicating with the issuing CA according to the configured connector when the status of the authentication certificate is queried; and retrieving the status of the authentication certificate; wherein the issuing CA and the connector are designated on a list of approved CAs in a configuration store.

The Koehler Patent

The Koehler patent discloses a method and system for authenticating digital certificates issued by an organization's authentication hierarchy. The system as

disclosed by the Koehler patent includes a verification server that manages a certificate repository and a verification cache having entries for verified digital certificates and certification revocation lists (abstract). The verification server as disclosed by the Koehler patent is a very basic certificate status responder. It only works with a single authentication hierarchy and obtains status from a certificate issuer's published certificate revocation lists (CRLs). When a subscriber query's for a certificate's status, if it is not already present in cache, the server checks the certificate issuer's CRL, caches the result for later use, and then reports certificate status. The status check includes verifying that the certificate is still valid by checking the authentication hierarchy of certificate signing chain. This result is also cached. Caching certificate status reduces overhead by reusing certificate status if already in cache. If it receives a status query that is later than the CRL publishing interval, a new CRL is retrieved and certificate status updated.

As disclosed by the Koehler patent, the verification server is limited in that it:

1. only works with a single authentication hierarchy;

2. only uses CRLs for obtaining certificate status; and

3. certificate status is not available for certificates issued after the publication time of the currently held CRL and will not become available until publication of the next CRL. The risk created by this gap in certificate status is not addressed by Koehler.

In contrast, Applicants have claimed a method of providing a Certificate Status Service ("CSS") for checking validities of authentication certificates issued by respective issuing Certification Authorities ("CAs") which:

1. is not a simple CRL based certificate status responder

2. works concurrently with multiple independent CAs and CA hierarchies and overcomes the limitations of CA bridging;

3. is compatible with all certificate status reporting means;

4. provides timely certificate status;

5. employs means to span communication outages and reduce communications loading, and for improving cache management and security;

6. uses business rules to enable CSS to include or exclude individual or group of CAs that are independent or exist within CA hierarchies ;

7. uses business rules to enable creation of layered risk based domains that can support a broad range of business applications; and

8. demonstrates how a trusted repository of information objects application uses CSS to create an authoritative copy of an information object that may require treatment as a transferable record.

Applicants' claimed methods and certificate status service encompass a solution to these and other problems not addressed by the Koehler patent. For example, as encompassed by the Applicants' claimed method, a certificate status service (CSS) can obtain certificate status by interoperating with multiple independent Certificate Authorities (CAs) and their hierarchies. The CSS implements multiple certificate status retrieval methods, most of which, unlike CRLs, report more timely status. Applicants' claimed solution would not have been obvious to one of ordinary skill based on the Koehler patent. None of the multiple US Government Agency or International Standard Groups (e.g., ITU, ISO, Internet Engineering Task Force (IETF)) efforts to bridge CA hierarchies have been successful at the time of

Applicants' invention. Rather, the state of the art at the time of Applicants' invention was aimed more at creating a single ubiquitous certificate status reporting protocol.

Applicants' claimed certificate status service (CSS) succeeds in providing a practical means for interoperating in an environment where multiple independent CAs and CA hierarchies exist with dissimilar trust policies and practices, and different certificate status reporting means and communications implementations. Applicants' disclosed CSS uses CA vetting procedures and business rules to form multiple risk based domains that can support different operational and business requirements.

A second aspect of Applicants' claimed methods and certificate status service, not taught or suggested by the Koehler patent, is a trusted repository that utilizes the CSS to check certificate status while verifying multi-party digital signature blocks associated with authenticated information objects. Another aspect of Applicants' claimed methods and certificate status service is the use of a number of mechanisms (e.g., time-to-live, last-used, least-used, and use-counter data elements; validity period checking), to bridge communications outages, reduce computational overhead, better manage and optimize cache memory, and help mitigate risk. Koehler only requires that the certificate that is being checked be issued prior to when the next CRL due to be published and that all CAs in the signing chain above the issuing CA are still valid.

Regarding claim 1, the Examiner asserts on page 2 of the Office Action that the Koehler patent discloses "a method of providing a Certificate Status Service ("CSS") for checking validities of authentication certificates issued by respective issuing Certification Authorities ("CAs"), comprising the steps of: identifying

information needed for retrieving a status of an authentication certificate from an issuing CA that issued the authentication certificate." Applicants respectfully disagree. The Koehler patent discloses at col. 5, lines 14-20, a certificate content that in itself does not contain the necessary information as featured in Applicants' claimed methods and certificate status service to retrieve certificate status from multiple individual CAs or CA hierarchies. Accordingly, the Koehler patent would not have taught or suggested identifying information needed for retrieving a status of an authentication certificate from an issuing CA that issued the authentication certificate, as recited in claim 1.

Regarding claim 1, the Examiner further asserts on page 2 of the Office Action that the Koehler patent discloses "configuring a connector based on the identified information for communicating with the issuing CA. Applicants respectfully disagree. The Koehler patent discloses at col. 5, lines 46-50, that the verification server receives a plurality of client requests, which does not relate to communication information required to communicate with different independent CAs/CA hierarchies.

Regarding claim 1, the Examiner further asserts on page 2 of the Office Action that the Koehler patent discloses "communicating with the issuing CA according to the configured connector when the status of the authentication certificate is queried. Applicants respectfully disagree. The Koehler patent disclosure relies on the issuing CA publishing CRLs (col. 5, lines 53-55). In contrast, Applicants' claim 1 encompasses querying the issuing CA for certificate status using whatever certificate status means the CAs employ.

Regarding claim 1, the Examiner further asserts on page 3 of the Office Action that the Koehler patent discloses "retrieving the status of the authentication

certificate." Notwithstanding the Examiner's assertion, Applicants' claimed retrieval of the status of authenticating certificate is not taught or suggested by the prior art in that its risk management means and business rules can force status updates or clearing of status based on the number of times a certificate's' status is queried, or other criteria, which may differ based on community or application.

Regarding claim 1, the Examiner further asserts on page 3 of the Office Action that the Koehler patent discloses "wherein the issuing CA and the connector are designated on a list of approved CAs in a configuration store." Notwithstanding the Examiner's assertion, the Koehler patent is only valid for certificates issued in a single authentication hierarchy. The Koehler patent does not teach including or excluding an individual CA or CA hierarchy, and the Koehler patent did not suggest the recited claim features.

Regarding claim 2, the Examiner asserts on page 3 of the Office Action that the Koehler patent discloses the method of claim 1, wherein a local date and time are checked for whether they fall within a validity period indicated in the authentication certificate. Notwithstanding the Examiner's assertion, the Koehler patent discloses timestamps used to indicate when a cached certificate's status was verified. The Koehler patent would not have taught or suggested checking to see if local time is beyond the certificate's validity period as encompassed by Applicants' claim 2.

Regarding claim 3, the Examiner asserts on page 3 of the Office Action that the Koehler patent discloses the method of claim 1, wherein the issuing CA is included in the list of approved CAs by vetting and approving the issuing CA according to predetermined business rules, and if the issuing CA is vetted and not

approved, the issuing CA is designated on a list of not-approved CAs in the configuration store. Applicants respectfully disagree. The Koehler disclosure does not relate to maintaining a list of approved and disapproved CAs. The Koehler patent would not have taught or suggested excluding specific CAs. Rather, as disclosed by the Koehler patent, any CA in the authentication hierarchy is acceptable as long as its certificate has not been revoked and has not expired.

Regarding claim 4, the Examiner asserts on page 3 of the Office Action that the Koehler patent discloses the method of claim 3, wherein vetting and approving the issuing CA includes registering a representation of a trusted authentication certificate with the CSS and adding at least the representation, status and a time-to-live data element to a local cache memory, and a connector is configured for retrieving the added status when the status of the trusted authentication certificate is queried. Applicants respectfully disagree. The Koehler disclosure does not relate to vetting, approving, documenting, and implementing means of communicating with approved CAs to retrieve queried certificate's status. Rather, the Koehler disclosure as relied upon by the Examiner relates to stepping through the authentication hierarchy to check that the issuing CA's certificate is still valid and checking to see if the cached CRL is still valid.

Regarding claim 5, the Examiner asserts on page 4 of the Office Action that the Koehler patent discloses the method of claim 2, further comprising the steps of checking a local cache memory for the status, and if the status is found in the local cache memory and the local date and time are within the validity period, retrieving the status from the local cache memory, wherein if the status is not found in the local cache memory ...the CSS establishes a communication session with a certificate

status reporting component of the issuing CA, composes a certificate status request according to the configured connector, retrieves the status from the certificate status reporting component, closes the communication session with certificate status reporting component, and adds at least the authentication certificate's identification, status, and time-to-live to the local cache memory. Applicants respectfully disagree. The Koehler patent discloses cache storage of authenticated digital certificates or CRLs and a timestamp indicating when either was verified. In contrast, as encompassed by Applicants' claim 5, a certificate identifier, the result of the status check, and a time-to-live indicator are stored in a cache memory. Applicants' claimed features support a wide variety of certificate status protocols. The Koehler disclosure of a verification timestamp would not have taught or suggested the claimed time-to-live indicator with the CSS enforced policies and practices, and/or communications load mitigation.

Regarding claim 6, the Examiner asserts on page 4 of the Office Action that the Koehler patent discloses the method of claim 1, wherein the certificate status is indicated by a Certificate Revocation List (CRL), according to a publication schedule of the issuing CA, the CSS retrieves the CRL from a certificate status reporting component listed in the configuration store, the CSS clears a cache memory associated with the issuing CA, and the CSS determines the status of the authentication certificate from the CRL and stores the status in the cache memory associated with the issuing CA. Applicants respectfully disagree. The Koehler disclosure uses an initialized timestamp to ensure that the most current certificate status is used. This timestamp is updated on verify to ensure that the latest status is used for any item queried. In contrast, Applicants' claim 5 encompasses using CRLs

and any other certificate status reporting protocols. Applicants' claim 5 encompasses retrieving status or a CRL based on a certificate status query in which a number of algorithms can be employed to optimize cache and reduce system overhead (e.g., CRLs and any derived certificate statuses are removed based on the CRL publication interval).

Regarding claim 7, the Examiner asserts on page 4 of the Office Action that the Koehler patent discloses the method as claimed. The Koehler patent is silent on ΔCRL retrieval and processing as claimed.

Regarding claim 8, the Examiner asserts on page 5 of the Office Action that the Koehler patent discloses the method of claim 1, wherein the communicating step includes communicating according to a sequence of connectors. Applicants respectfully disagree. The Koehler disclosure relates to verifying the authentication hierarchy certificate chain and have nothing to do with connectors to communicate with multiple independent CAs. The Koehler patent would not have taught or suggested the claimed features.

Regarding claim 9, the Examiner asserts on page 5 of the Office Action that the Koehler patent discloses the method of claim 1, wherein a connector embeds more than one certificate status check in a single communicating step. Applicants respectfully disagree. The Koehler patent exclusively uses the CRLs certificate status reporting means. In contrast, claim 9 encompasses employing communications overhead reduction techniques such as nesting certificate status requests for a multi-party transaction where at least two parties have certificates issued by the same CA.

Regarding claim 10, the Examiner asserts on page 5 of the Office Action that the Koehler patent discloses the method of claim 1, wherein the authentication certificate is not used for identification. Applicants respectfully disagree. The Koehler disclosure addresses the use of certificate status as it pertains to verifying digital signatures. In contrast, Applicants' claim 10 encompasses CSS which supports certificates used for purposes other than proof of identity such as attributes certificates or certificates used for encrypting storage media.

Regarding claim 11, the Examiner variously asserts on page 5 of the Office Action that the Koehler patent discloses the claimed method of retrieving a status of an authentication certificate. Applicants respectfully disagree. The Koehler patent is silent on a trusted third-party repository of information objects that is a trusted repository of information objects. In contrast, applicants' claim 11 encompasses an application where interacting parties may use certificates issued by independent CAs and/or CAs from different CA hierarchies, but where the ability to trust the identity of the participants as conveyed in their authentication certificates is paramount. The Kohler disclosure deals with the verification server maintaining status in a cache and has nothing to do with a configuration store that maintains all information necessary to obtains certificate status from any known and approved CA or certificate status reporting service. The Koehler reference first looks in cache for an item's status and reports status if an entry is found, otherwise it creates an entry and retrieves status, prior to reporting status. In contrast, Applicants' claim 11 encompasses using the current CRL stored in local storage to simply report status based on whether the certificate is identified in the list. Further, the Koehler patent is silent as to how the

status is obtained from CAs that are not a member of the CA hierarchy or that are a certificate status reporting service other than a CA.

Further regarding claim 11, the Koehler disclosure deals with verifying the CA certificate chain. This test validates whether the issuing CA within the chain can be trusted. Since the response to a certificate status query may be in any number of status reporting protocols, Bisbee must interpret the response to extract the status contained therein. The Koehler timestamp indicates the time of verification. In contrast, Applicants' claim 11 encompasses time-to-live value being set based on CSS policy and indicates when the status value is to be erased from cache. Applicants' business rules can indicate a shorter time-to-live value is to be used, such as where issued certificates are associated with high value transactions. The Koehler patent doesn't disclose making use of a time-to-live value, and adds the validated certificate itself to cache. The Koehler patent merely gives an overview of an authentication hierarchy. The Koehler patent would not have taught or suggest the CSS being used by a trusted third-party repository of information objects for obtaining certificate status, as recited in claim 11.

Regarding claim 15, the Examiner variously asserts on page 7 of the Office Action that the Koehler patent discloses the claimed method. Applicants respectfully disagree. The Koehler patent describes how to walk the certificate signing chain to authenticate the CA's CRL, not use of a CRL to check an issued certificate's status. The Koehler patent is silent as to clearing of status based on a CSS's certificate status retention policy and business rules. The Koehler patent is silent as to the use of a real-time certificate status reporting protocol to retrieve certificate status for a CA or certificate status reporting service. The Koehler patent would not have taught or

suggested the features of providing a status of an authentication certificate as indicated by a Certificate Revocation List ("CRL") when the certificate's issuing CA uses CRLs for indicating status; otherwise, providing the status indicated by a cache memory when the cache memory includes a status and a time-to-live data element is not exceeded; if the time-to-live data element is exceeded, clearing the status from the cache memory; requesting and retrieving the status using a real-time certificate status reporting protocol when the status is not in the cache memory; adding at least the certificate's identification, status, and time-to-live data element to the cache memory; and providing the retrieved status, as recited in claim 15.

Regarding claim 19, the Examiner asserts on page 7 of the Office Action that the Koehler patent discloses the method executing a transaction as recited in claim 19. Applicants respectfully disagree. The Koehler patent describes a three level authentication hierarchy. In contrast, Applicants' claim 19 encompasses a trusted third-party repository's processing and handling of authenticated information objects, where a first party (owner) instructs the trusted third-party repository of information objects to transfer ownership and control to a second party (new owner). The Koehler patent is silent as to the execution of multiparty transactions. The Koehler patent is silent on the use of the CSS (certificate status checking) by a trusted third-party repository of information objects to obtain certificate status for digital signature blocks affixed to authenticated information objects that are received by the trusted third-party repository of information objects and the trusted third-party repository's handling of the authenticated information object based on the certificate status returned by the CSS. The Koehler patent would not have taught or suggested retrieving an authenticated information object from a trusted repository, ...the

authenticated information object is stored as an electronic original information object under the control of the trusted repository; executing the retrieved authenticated information object by the second party by including in the retrieved authenticated information object a third digital signature block comprising at least a third digital signature and a third authentication certificate of the second party; and forwarding the executed retrieved authenticated information object to a trusted third-party repository of information objects, wherein the trusted third-party repository of information objects verifies digital signatures and validates authentication certificates associated with the digital signatures included in information objects by at least retrieving status of the authentication certificates from a Certificate Status Service ("CSS") provided according to claim 1, as recited in claim 19.

Regarding claim 22, the Examiner asserts on page 9 of the Office Action that the Koehler patent discloses the method of claim 19, wherein if the trusted third-party repository of information objects rejects a digital signature block, the trusted third-party repository of information objects requests a remedy that requires the digital signature to be recomputed and the signature block to be reforwarded. Applicants respectfully disagree. The Koehler patent describes verification of a CA certificate in an authentication hierarchy and is silent on a trusted third-party repository of information objects requiring resubmission of any information object to be authenticated that does not have valid signature blocks. The Koehler patent would not have taught or suggested the features recited in claim 22.

Regarding claim 23, the Examiner asserts on page 9 of the Office Action that the Koehler patent discloses the method of claim 19, wherein the trusted third-party repository of information objects checks the local date and time for accuracy and that

they are within a validity period indicated by the second party's authentication certificate. Notwithstanding the Applicants' assertions, the Koehler disclosure merely relates to validating the CA authentication hierarchy certificate signing chain. In contrast, Applicants' claim 23 encompasses a trusted repository that holds authenticated information objects that may be authoritative copies. It can do simple certificate validity period checking without use of any external service. As encompassed by Applicants' claim 23, both the CSS and trusted third-party repository of information objects use certificate validity period testing. The trusted third-party repository's use is intended to reduce interactions with the CSS. Koehler uses this test, but the specific reference refers to validating the CA authentication hierarchy certificate signing chain. The Koehler disclosure would not have taught or suggested these capabilities encompassed by claim 23.

Regarding claim 26, the Examiner asserts on page 9 of the Office Action that the Koehler patent discloses the method of 19, wherein one or more digitized handwritten signatures are included in the information object, and placement of the digitized handwritten signatures in a data structure is specified by at least one signature tag. Applicants respectfully disagree. The Koehler patent is silent on the use and placement of digitized handwritten signatures.

Regarding claim 27, the Examiner asserts on page 9 of the Office Action that the Koehler patent discloses the method of claim 26, wherein one or more signature blocks are separately forwarded to the trusted third-party repository of information objects with respective signature tags, and the trusted third-party repository of information objects validates the signature blocks. Applicants respectfully disagree. The Koehler patent is silent on a trusted third-party repository of information objects

that is a secure repository of information objects and that separately verifies digital signatures on submitted information objects prior to storing and controlling these information objects. The Koehler patent is silent on detaching signature blocks from content and forwarding only the signature block to the trusted third-party repository of information objects. Further, Koehler patent is silent on the handling and processing of detached signature blocks. The Koehler patent is silent on a trusted third-party repository of information objects using a wrapper or placement of signature blocks and information objects in wrappers.

Regarding claim 28, the Examiner asserts on page 10 of the Office Action that the Koehler patent discloses the method of claim 27, wherein the trusted third-party repository of information objects verifies a digital signature and validates an authentication certificate in a signature block. Applicants disagree. The Koehler patent is silent on business rules or their use by the trusted third-party repository of information objects to check the authority of the identified party to perform actions. The Koehler patent is silent on the need for the trusted third-party repository of information objects to check the accuracy of local time. The Koehler patent merely refers to methods for reducing computational overhead, and cache management and housekeeping of certificate status entries. In contrast, Applicants' claim 28 encompasses steps to validate signature blocks. The Koehler patent describes verification server verification process, but the Koehler patent does not relate to transaction processing.

Regarding claim 29, the Examiner asserts on pages 10 and 11 of the Office Action that the Koehler patent discloses the method of claim 19, wherein the CSS provides authentication certificate status to the trusted third-party repository of

information objects by at least the steps of checking a local cache memory for the status, and if the status is found in the local cache memory and the local date and time are within the validity period, and retrieving the status from the local cache memory; if the status is not found in the local cache memory or if the local date and time are not within the validity period, the CSS establishes a communication session with a certificate status reporting component of the issuing CA, composes a certificate status request according to the configured connector, retrieves the status from the certificate status reporting component, closes the communication session with certificate status reporting component, and adds at least the authentication certificate's identification, status, and a time-to-live data element to the local cache memory. Applicants respectfully disagree. The Koehler verification server caches authentication certificates or CRLs for a single CA hierarchy and efficiently manages entries and certificate status for that hierarchy. In contrast, Applicants' claim 29 encompasses concurrently retrieving certificate status from any approved CA that has been previously configured.

Regarding claim 30, the Examiner asserts on page 11 of the Office Action that the Koehler patent discloses the method of claim 19, wherein the first party is a first trusted third-party repository of information objects and the transaction is for transferring custody of one or more electronic originals to the first trusted third-party repository of information objects from a second trusted third-party repository of information objects, an owner of the transaction provides the second trusted third-party repository of information objects with a manifest that identifies electronic originals to be transferred to the first trusted third-party repository of information objects, the second trusted third-party repository of information objects establishes

communication with the first trusted third-party repository of information objects and identifies the purpose of its actions, the manifest is communicated to the first trusted third-party repository of information objects so that it is able to determine when the transfer of custody has been completed, the second trusted third-party repository of information objects transfers each identified electronic original to the first trusted third-party repository of information objects, the first trusted third-party repository of information objects retrieves status of the second trusted third-party repository's certificate and verifies the second trusted third-party repository's digital signature on each transferred electronic original, if any of the second trusted third-party repository's digital signatures or certificates are invalid, then the first trusted third-party repository of information objects notifies the second trusted third-party repository of information objects and seeks a remedy, if the second trusted third-party repository of information objects does not provide a remedy, the first trusted third-party repository of information objects notifies the transaction owner that the requested transfer of custody has failed, otherwise the second trusted third-party repository of information objects creates a new wrapper for each successfully transferred information object, adding a date-time stamp and the first trusted third-party repository's signature block. Applicants respectfully disagree. The Koehler patent is silent on validation of the initiating instruction and transfer-of-custody of authenticated information between trusted third-party repositories.

Regarding claim 31, the Examiner asserts on page 12 of the Office Action that the Koehler patent discloses the method of claim 30, wherein the transaction is a transfer of ownership in response to an instruction, transfer of ownership documentation is placed in either the first trusted third-party repository of information

objects or the second trusted third-party repository of information objects, the trusted third-party repository of information objects having the transfer of ownership documentation validates authenticity of the transfer of ownership documentation by verifying all digital signatures, certificate validity periods, and using the CSS to check certificate status of all authentication certificates included in the transfer of ownership documentation, appends a date and time indication, and digitally signs, wraps and stores the transfer of ownership documentation, which are added to the manifest. Applicants disagree. The Koehler patent is silent on validation of the initiating instruction and transfer-of-ownership of authenticated information objects.

The Konheim, Kocher and Smithie Patents

The Konheim, Kocher and Smithie patents do not cure the deficiencies of the Koehler patent. Rather, these secondary references were applied in combination with the Koehler patent to variously reject dependent claims.

For the foregoing reasons, Applicant's independent claims 1, 11 and 15 are allowable. The remaining claims depend from the respective independent claims and recite additional advantageous features which further distinguish over the documents relied upon by the Examiner. As such, the present application is in condition for allowance.

All objections and rejections raised in the Office Action having been addressed, it is respectfully submitted that the application is in condition for allowance and a Notice of Allowance is respectfully solicited.

Respectfully submitted,

BUCHANAN INGERSOLL & ROONEY PC

Date: October 3, 2006

By: _____
Richard J. Kim
Registration No. 48360

P.O. Box 1404
Alexandria, VA 22313-1404
703 836 6620